Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

EAVESDROPPING ATTACK IN INDUSTRIAL WIRELESS SENSOR NETWORK ON INTERCEPTED SIGNAL

Hafsa Maseera [1] | M. Narayana [2]

[1] Student, Department of Electronics and Communication Engineering, Jayaprakash Narayana College of Engineering, Mahabubnagar, India.

[2] Professor and HOD, Department of Electronics and Communication Engineering, Jayaprakash Narayana College of Engineering, Mahabubnagar, India.

ABSTRACT

This paper studies the intercept behavior of associate industrial wireless device network (WSN) consisting of a sink node associated multiple sensors within the presence of an eavesdropping offender, wherever the sensors transmit their detected info to the sink node through wireless links. As a result of the printed nature of radio radiation propagation, the wireless transmission from the sensors to the sink is pronto overheard by the snoop for interception functions. In associate information-theoretic sense, the secrecy capability of the wireless transmission is that the distinction between the data rate of the most link (from device to sink) which of the wiretap link (from device to eavesdropper). If the secrecy capability becomes non-positive as a result of the wireless weakening result, the sensor's information transmission might be with success intercepted by the snoop associated an intercept event happens during this case. However, in industrial environments, the presence of machinery obstacles, tinny frictions and engine vibrations makes the wireless weakening fluctuate drastically, leading to the degradation of the secrecy capability. As a consequence, associate optimum device planning theme is projected during this paper to shield the legitimate wireless transmission against the eavesdropping attack, wherever a device with the best secrecy capability is regular to transmit its detected info to the sink. Closed-form expressions of the chance of incidence of associate intercept event (called intercept probability) are derived for the standard round-robin planning and also the projected optimum planning schemes. Also, associate straight line intercept chance associate analysis is conducted to supply an insight into the impact of the device planning on the wireless security. Numerical results demonstrate that the projected device planning theme outperforms the standard round-robin planning in terms of the intercept chance.

KEY WORDS: Intercept behavior, industrial wireless sensor networks, sensor scheduling, intercept probability, Nakagamifading.

1. INTRODUCTION:

In industrial WSNs, as a result of the published nature of radio propagation, the wireless medium is hospitable be accessed by each licensed and unauthorized users [1], leading WSNs to be a lot of susceptible to the eavesdropping attack than wired device networks, wherever communication nodes area unit physically connected with wire cables and a node while not being connected is unable to access for contraband activities [2], [3]. To be specific, as long as a listener hides within the industrial WSNs, [4], [6] the legitimate wireless transmissions among the sensors may be pronto overheard by the listener, [7] which can decode its broach transmissions and violate the confidentiality of the sensors' info communications [8]. Therefore, it's of prominence to research the protection of business WSNs against the eavesdropping attack.

Traditionally, the science techniques were oppressed to shield the wireless communications against eavesdropping, which generally place confidence in secret keys and might stop associate hearer with restricted machine capability from intercepting the info transmission between wireless sensors. However, associate hearer with unlimited computing power remains able to crack the encrypted information communications with the help of complete key search (known because the brute-force attack) [9],[10]. Moreover, the key distribution and agreement between the wireless sensors exhibit varied vulnerabilities and more increase the protection risk. To the present finish, physical-layer security is rising as a promising paradigm for secure communications by exploiting the physical characteristics of wireless channels, which may effectively shield the confidentiality of communication against the eavesdropping attack, even with unlimited machine power [11].

The physical-layer security work was pioneered by Claude Shannon [12]and extended by Wyner [13], wherever Associate in Nursing information-theoretic framework was established by developing possible secrecy rates for a classical wiretap channel model consisting of 1 supply, one destination Associate in Nursing a hearer. The alleged secrecy capability [14] was shown because the distinction between the data rate of the most link from supply to destination which of the wiretap link from supply to hearer. If the secrecy capability becomes non-positive (i.e., the data rate of the most link becomes smaller compare to that of the wiretap link), the hearer can reach intercepting the supply message Associate in nursing an intercept event is taken into account to occur during this case. This means that increasing the secrecy capability will effectively decrease the chance that the hearer with success intercepts the supply message [15,16]. However, the secrecy capability of wireless-transmission is severely restricted owing to the wireless attenuation result. Moreover, the presence of machinery obstacles, antimonial frictions and engine vibration in industrial environments makes the wireless attenuation fluctuate drastically, leading to an extra degradation of the secrecy capability.

To overcome this limitation, significant analysis efforts are dedicated to increase the secrecy capability of the wireless transmission through the bogus noise generation [17,18]. the bogus noise assisted security approaches permit the legitimate transmitters to get a specifically designed intrusive signal (called artificial noise) such solely the listener is adversely full of the bogus noise, whereas the supposed receiver remains unaffected. This results in a degradation of the wiretap link in terms of the data rate while not moving the data rate of the most link, leading to Associate in Nursing raised secrecy capability. The authors thought of the utilization of multiple antennas for generating the bogus noise and showed that the quantity of an antennas at the legitimate transmitter ought to be over that at the legitimate receiver for the sake of making certain that the most link is unaffected by the bogus noise. Added to this, Goeckel [19] investigated the utilization of cooperative relays for the bogus noise generation and incontestable a major security improvement in terms of the secrecy capability.

The main contributions of this paper are summarized as follows. First, associate optimum detector programming theme is projected for shielding the economic wireless transmission against the eavesdropping attack, wherever a detector with the very best secrecy capability is chosen to transmit its perceived info to the sink. the standard round-robin programming is additionally thought-about as a benchmark. Second, closed-form expressions of the intercept likelihood for the standard round-robin programming and also the projected optimum detector programming schemes are derived in Nakagami attenuation environments. Third, associate straight line intercept likelihood analysis is conducted and the diversity order of the projected programming theme is shown because the total of Nakagami shaping factors of the most links from the sensors to the sink. Finally, numerical results show the advantage of the projected detector programming theme over the standard round-robin programming in terms of the intercept likelihood.

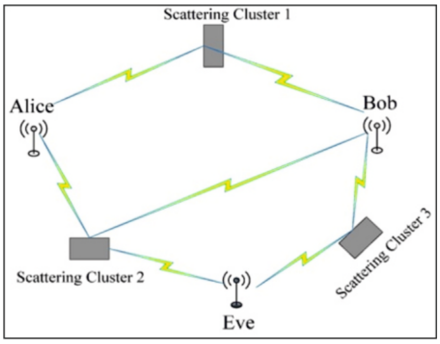


Fig 1: Industrial WSN with source, destination and eavesdropper

Existing system:
However, the secrecy capability of wireless transmission is severely restricted owing to the wireless attenuation impact. Moreover, the presence of machinery obstacles, gold-bearing frictions and engine vibration in industrial environment makes the wireless attenuation fluctuate drastically, leading to an extra degradation of the secrecy capability.

There by multiple relay nodes existing, the relay choice for wireless security augmentation, wherever the relay node that may attain the very best secrecy con to eavesdropping is chosen because the "best" relay to help the source-destination transmissions.

Traditionally, the science techniques were exploited to safeguard the wireless communications against eavesdropping, which generally deem secret keys and may forestall associate attender with unlimited ready to crack the encrypted information communications with aid key search brute-force attack

If the secrecy capability becomes non-positive (i.e., the data rate of the most link becomes lesser that of the wiretap link), the snooper can achieve intercepting the supply message and an intercept event is taken into account to happens. More specifically, in industrial WSNs, the wireless channel is difficult as a result of the machinery obstacles, bimetallic frictions and engine vibrations. This motivates North American country to contemplate the employment of a posh weakening model for characterizing the economic wireless channel, rather than a less complicated Third Baron Rayleigh weakening model used.

Finally, we will improve the physical layer security with exploitation of device programing theme.

Disadvantages:
Secure is very less
Bandwidth waste
Much than artificial noise generates.

Proposed System:
Moreover, the key allocation and contract between the wireless sensors show varied vulnerabilities and advance increase the safety risk.

In this project, we tend to investigated the utilization of device programming to enhance the physical-layer security of commercial WSNs against the eavesdropping attack associated projected a best device programming theme, aiming at maximizing the secrecy capability of wireless transmissions from sensors to the sink.

First, improve the wireless physical-layer security with aid of sensing element programing theme. so as to effectively defend against the eavesdropping attack, the sensing element programing ought to take under consideration the channel state data (CSI) of each the most channel and wiretap channel, differing from the normal programing methodology, wherever solely the CSI of main channel is taken into account for the turnout maximization.

Finally, associate degree optimum detector planning theme is projected for safeguarding the commercial wireless transmission against the eavesdropping attack, wherever a detector with the best secrecy capability is chosen to transmit its detected info to the sink. the standard round-robin planning is additionally thought-about.

Advantages:
High security
Increase throughput level.
Avoided the interference.

2. MATERIAL AND MODEL:

we consider an industrial WSN consisting of a sink node and N sensors in the presence of an eavesdropper, where all nodes are assumed with single antenna and the solid and dash lines represent the main link and wiretap link, respectively. Notice that the eavesdropper could be either an illegitimate user or a legitimate user who is interested in tapping other users' data information [21], [22] For notational convenience, N sensors are denoted by $S = \{s\,i \mid i = 1, 2, \cdots, N\}$.

In the industrial WSN of, N sensors communicate with the sink using an orthogonal multiple access method such as the time division multiple access (TDMA) and orthogonal frequency division multiple access (OFDMA). When a sensor (e.g., s i) is scheduled to transmit its data to the sink over a channel (e.g., a time slot in TDMA or an OFDM subcarrier in OFDMA), the eavesdropper attempts to intercept the information transmitted from s i. Traditionally, given an orthogonal channel, a node with the highest data throughput is typically selected among N sensors to access the given channel and to communicate with the sink, which aims at maximizing the transmission capacity without considering the eavesdropping attack. By contrast, this paper is focused on improving the wireless physical-layer security with the aid of sensor scheduling. In order to effectively defend against the eavesdropping attack, the sensor scheduling should take into account the channel state information (CSI) of both the main channel and wiretap channel, differing from the traditional scheduling method, where only the CSI of main channel is considered for the throughput maximization.

2.1: Modules:

To make our project as efficient we divided our total project into small modules. There are given as below.

- 1. Sensor Scheduling
- 2. Security

1. *Sensor Scheduling:*
The Sensor selection problem arises when multiple sensors are jointly trying to estimate a process but only a subset of them can take and/or use measurements at any time step.

2. *Security:*
Moreover, the wireless communication are employed by sensor network felicitates eavesdropping and packet injection by an advisory.

2.2: Algorithm:

```
1)  If node has data
      a. Check the routing table
         i. If route found
            1. Forward the data
            2. Start Counting data
            3. At beginning of data count set the timer to check the counting

         ii. If route not found
            1. Generate the req on demand routing protocol
            2. Update the request with own public key
            3. Broadcast to all neighbor to find destination

2)  If Req received
      a. Checks whether req is new
         i. If not
            1. Ignore

         ii. If yes
            1. Updates the reveres route
            2. Updates the key information
            3. Checks whether node is the destination

      a. If yes
         i. Generate the rep with its  own public key

      b. If not
         i. Forward the packet

3)  If Rep received
      a.  Updates reverse route

      b.  Updates the key information

      c.  Checks node has data to send to source
          i. If yes
             1. Go to main step

      a. Checks the route to rep destination
         i.  If found
             1. Send
        ii.  Else
             1. Ignore

4)  If data received
      a. Checks I'm the destination
         i.  If yes
             1. Generate the ack

      a. Set current time as ack time Ta

      b. Checks the pair-wise key b/w source and destination
         i. If found set key as $K_{S_{s-d}}$

c.    Split Ta into separate character  $\cup T_{sA}$

d.    Create empty list for encrypted data El

e.    For-each char $Pt \in T_{sA}$
      i. Encrypt by AES algorithm
         1. Pt=>Ct
         2. Convert to ascii value Cta
         3. Generate random number(rand)
         4. New value Nv=Cta-rand
         5. (Cta&Nv&rand) $\cup El$
            i. Make digital sign
               1. Checks for own private key
        2. For_each value of El

a.   Extract Nv

b.   Encrypt by RSA private key
     I. Nv==>CNv
     ii. CNv U Digital_sgn_lst
        2.Send the secrete ack with

a.   Digital sign

b.   Rand number

c.   Generation time

If digital sign received in source

a.   Node checks the public key info for ack generator
     i. If found
       1. decrypt by Pu Key ===>Ptrsa
       2.  Checks for secrete pair key

a.   If found
     i. Decrypt Ptrsa by K_(S_(s-d) ) ==>Pt

     3. Pt U plain text list

b.   Compare with original form of digital sign with plain text list data
     i. If match
       1. Forward further data through same path

     ii. If not matched
       1. Switch to secure ack mode
```

2.3: Project requirements:
Hardware requirements:

- Single PC20 GB Hard disc space
- 1GB RAM

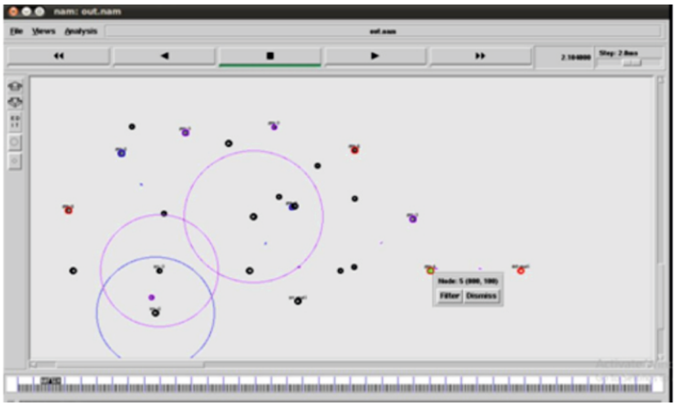
Software requirements:

- Linux OS (Ubuntu 10.04)
- NS2.34

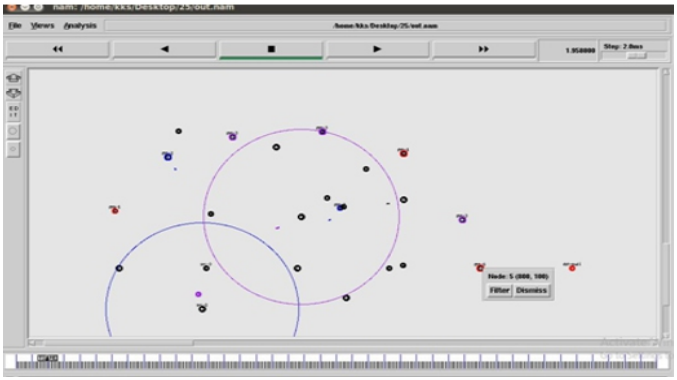
Language:

- TCL (Tool command Language)
- C++

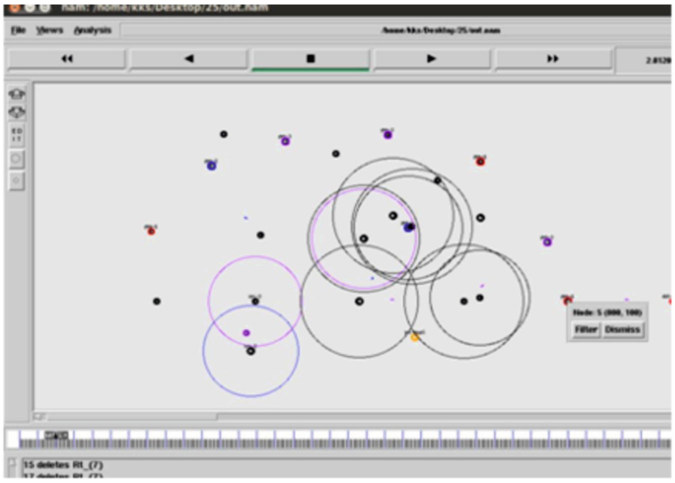
4. RESULT & DISCUSSION:
1.Existing Output:



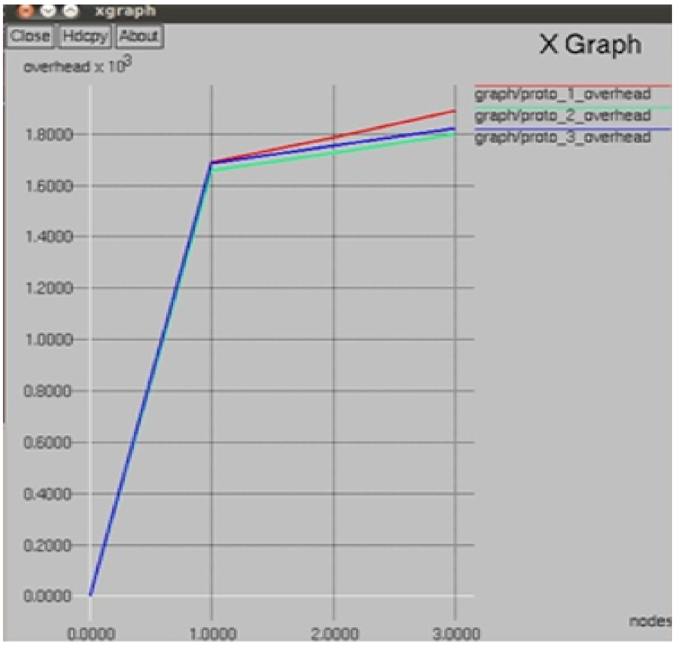
2. Proposed Output:



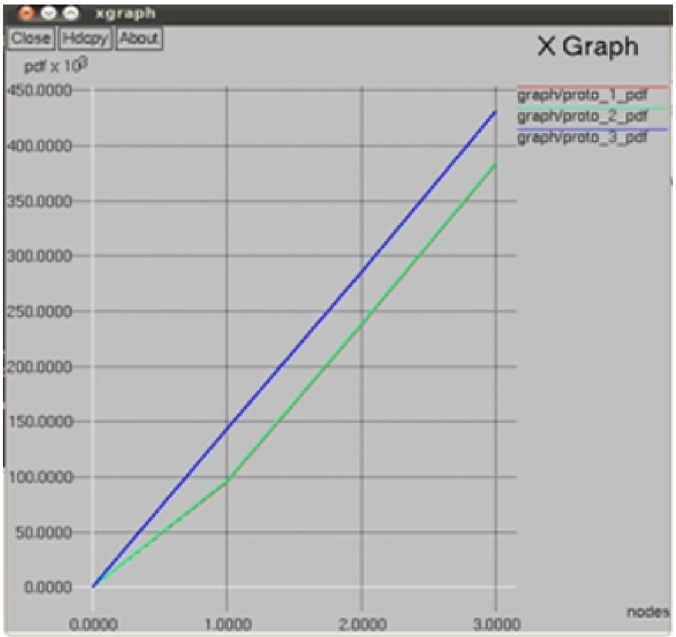
3. Enhanced Output:



4: Comparisons Graph:
A] Overhead:



B] Packet Delivery Ratio [PDF]:



5. CONCLUSION:

In this paper, we tend to investigated the employment of sensing element planning to improve the physical-layer security of commercial wireless sensor network counter to the eavesdropping attack and projected an optimal sensor scheduling theme, targeting to increase the secrecy-capacity of wireless transmissions from sensors to the sink. We additionally thought-about the traditional round-robin scheduling as a benchmark. we tend to derived precise closed-form expressions of the intercept chance for each the traditional round-robin planning and therefore the projected optimum planning schemes in Nakagami weakening environment. AN straight line intercept probability analysis was additionally bestowed to characterize the diversity gains of the round-robin planning and therefore the optimal sensor planning schemes. Numerical results validated that the projected optimum planning theme performs better than the traditional round-robin planning in terms of the intercept chance. Also, upon increasing the number of sensors, the intercept chance of the projected optimal sensor planning theme considerably decreases, showing the physical layer security enrichment of commercial WSNs.

REFERENCES:

[1] W. Shen, T. Zhang, F. Barac, and M. Gidlund, “PriorityMAC: A priority enhanced MAC protocol for critical traffic in industrial wireless sensorand actuator networks,” IEEE Trans. Industrial Informatics, vol. 10, no.1, pp. 824-835, Feb. 2014.

[2] J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang,“Mixed sound event verification on wireless sensor network for home automation,” IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 803-812, Feb. 2014.

[3] R. C. Luo and O. Chen, “Mobile sensor node deployment and asynchronous power management for wireless sensor networks,” IEEE Trans.Industrial Electronics, vol. 59, no. 5, pp. 2377-2385, May 2012.

[4] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter,“An experimental study of selective cooperative relaying in industrialwireless sensor networks,” IEEE Trans. Industrial Informatics, vol. 10, no. 3, pp. 1806-1816, Aug. 2014.

[5] O. Kreibich, J. Neuzil, and R. Smid, “Quality-based multiple-sensor fusion in an industrial wireless sensor network for MCM,” IEEE Trans.Industrial Electronics, vol. 61, no. 9, pp. 4903-4911, Sept. 2014.

[6] T. M. Chiwewe and G. P. Hancke, “A distributed topology controltechnique for low interference and energy efficiency in wireless sensor networks,” IEEE Trans. Industrial Informatics, vol. 8, no. 1, pp. 11-19, Feb. 2012.

[7] P. T. A. Quang and D.-S. Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks,” IEEE Trans. Industrial Informatics, vol. 8, no. 1, pp. 61-68, Feb. 2012.

[8] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Xu, “A reconfigurable smart sensor interface for industrial WSN in IoT environment ,” IEEE Trans. Industrial Informatics, vol. 10, no. 2, pp. 1417-1425 , May 2014.

[9] F. Gandino, B. Montrucchio, and M. Rebaudengo, “Key management for static wireless sensor networks with node adding,” IEEE Trans. Industrial Informatics, vol. 10, no. 2, pp. 1133-1143, May 2014.

[10] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” IEEE Trans. Industrial Informatics, vol. 9, no.1, pp. 277-293, Feb. 2013.

[11] Y. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” IEEE Network, vol. 29, no. 1, pp. 42-48, Jan. 2015.

[12] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, pp. 656-715, 1949.

[13] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Aug. 1975.

[14] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” IEEE Trans. Information Theory, vol. 24, pp. 451-456, Jul. 1978.

[15] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical-layer security in cooperative wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[16] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” IEEE Trans. Vehicular Technology, vol. 63, no. 6, pp. 2653-2661, Jun. 2014.

[17] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” IEEE Trans. Wireless Communications, vol. 7, no. 6, pp. 2180-2189, Jul. 2008.

[18] X. Zhou and M. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 3831-3842, Aug. 2010.

[19] D. Goeckel, et al., “Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 2067-2076, Oct. 2011.

[20] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” IEEE Trans. Communications, vol. 61, no. 12, pp. 5103-5113, Dec. 2013.

[21] D. Lee and B. J. Jeong, “Performance analysis of combining space-time block coding and scheduling over arbitrary Nakagami fading channels,” IEEE Trans. Wireless Communications, vol. 13, no. 5, pp. 2540-2551, May 2014.

[22] S. Hussain and X. N. Fernando, “Closed-form analysis of relay-based cognitive radio networks over Nakagami-m fading channels,” IEEE Trans. Vehicular Technology, vol. 63, no. 3, pp. 1193-1203, Mar. 2014.

[23] H. Dong, Z. Wang, J. Lam, and H. Gao, “Distributed filtering in sensor networks with randomly occurring saturations and successive packet dropouts,” International Journal of Robust and Nonlinear Control, vol. 24, no. 12, pp. 1743-1759, Aug. 2014.

[24] H. Dong, Z. Wang, and H. Gao, “Distributed H-infinity filtering for a class of Markovian jump nonlinear time delay systems over lossy sensor networks,” IEEE Trans. Industrial Electronics, vol. 60, no. 10, pp. 4665-4672, Oct. 2013.

[25] H. Dong, Z. Wang, and H. Gao, “Distributed filtering for a class of time-varying systems over sensor networks with quantization errors and successive packet dropouts,” IEEE Trans. Signal Processing, vol. 60, no. 6, pp. 3164-3173, Jun. 2012.

[26] J.-C. Chen, C.-K. Wen, and P. Ting, “An efficient pilot design scheme for sparse channel estimation in OFDM systems,” IEEE Communications Letters, vol. 17, no. 7, pp. 1089-7798, Jul. 2013.

[27] X. He, R. Song, and W.-P. Zhu, “Pilot allocation for sparse channel estimation in MIMO-OFDM systems,” IEEE Trans. Circuits and Systems II: Express Briefs, vol. 60, no. 9, pp. 612-616 , Sept. 2013.

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” IEEE Trans. Signal Processing, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[29] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[30] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” IEEE Trans. Inf. Theory, vol. 24, pp. 451–456, Jul. 1978.

[31] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, pp. 339–348, May 1978.

[32] Y. Liang, H. V. Poor, and S. Shamai, Information Theoretic Security.Delft, The Netherlands: Now Publishers, 2009.

[33] A. O. Hero, “Secure space-time communication,” IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[34] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas: The MISOME wiretap channel,” IEEE Trans. Inf. Theory, Aug. 2007. [Online]. Available: http://arxiv.org/abs/0708.4219, submitted for publication.

[35] R. Negi and S. Goelm, “Secret communication using artificial noise,” in Proc. IEEE Vehicular Tech. Conf., Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[36] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inf. Theory, Oct. 2007 [Online]. Available: http://aps.arxiv.org/abs/0710.1920, submitted for publication.

[37] T. Liu and S. Shamai, “A note on the secrecy capacity of the multi-antenna wiretap channel,” IEEE Trans. Inf. Theory, Nov. 2007 [Online]. Available: http://arxiv.org/abs/0710.4105, submitted for publication.

[38] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in Proc. IEEE Int. Symp. Inf. Theory, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[39] Z. Li, W. Trappe, and R. Yates, “Secret communication via multi-antenna transmission,” in Proc. 41st Conf. Information Sciences Systems, Baltimore, MD, Mar. 2007.

[40] S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007.